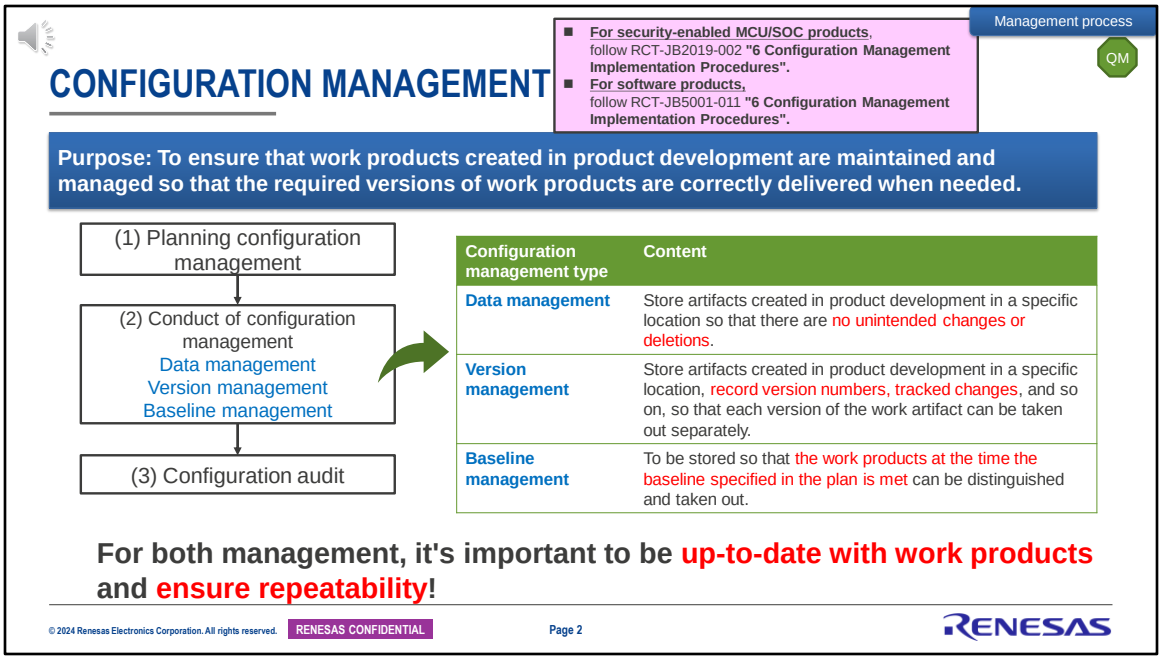
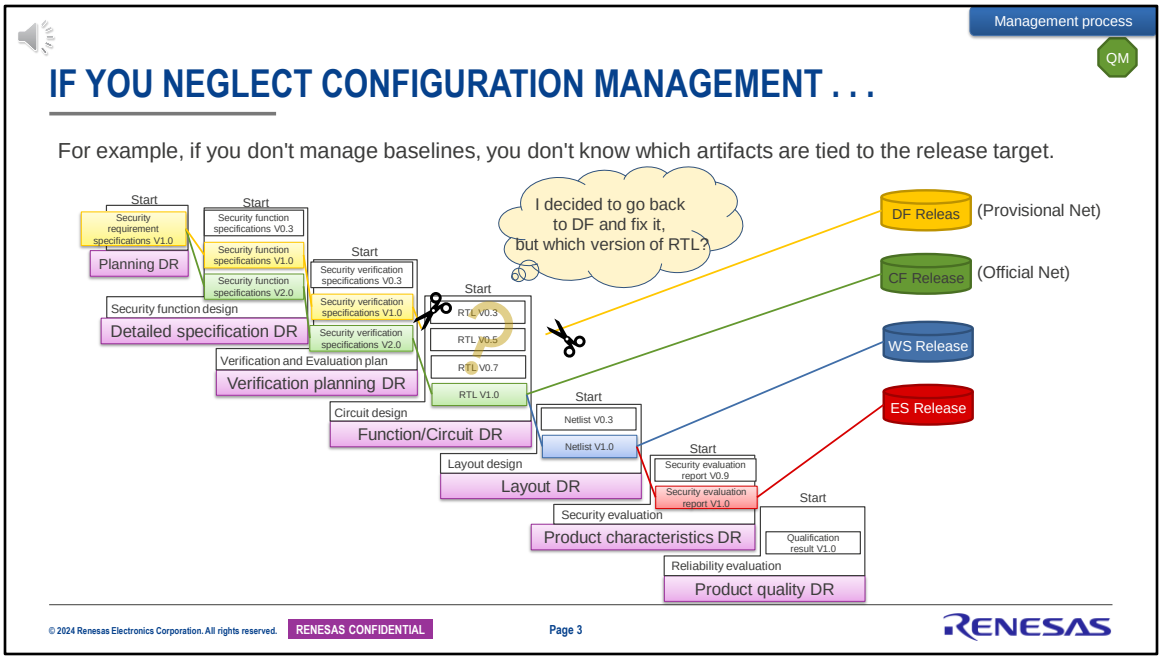
This video is a lecture video for the management process of security product development process.
The management process is common to all development processes: requirements management process, semiconductor product development process, and software product development process.

Now let's explain the management process.

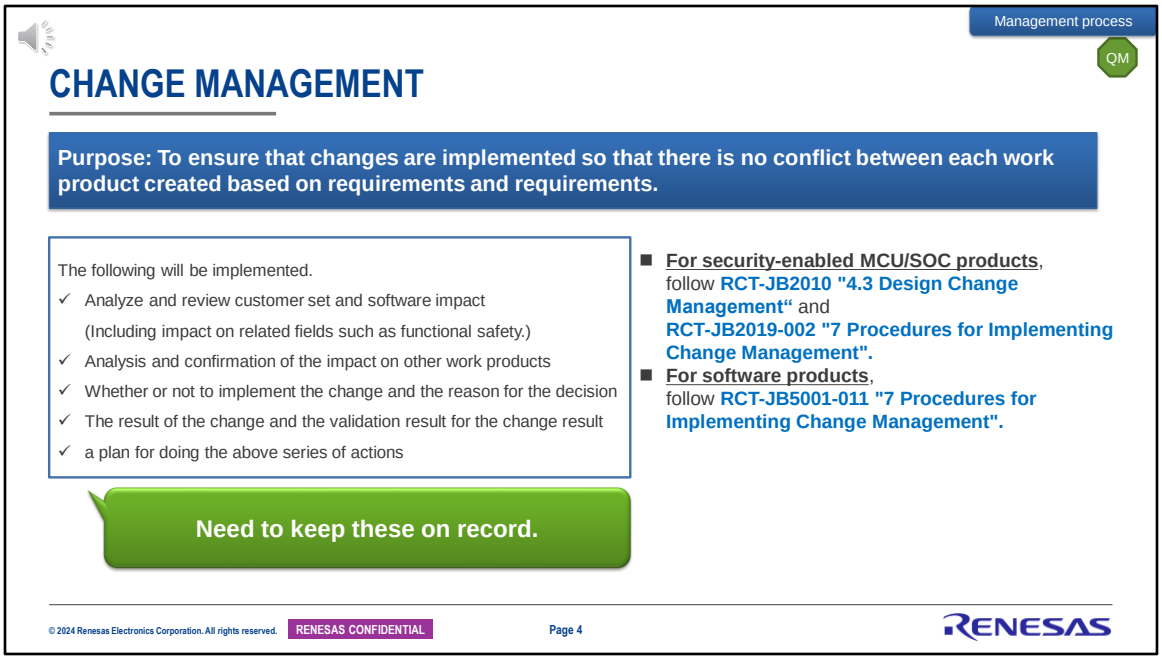


First is configuration management.
The purpose of configuration management is to ensure that the work products created are maintained and managed so that you can retrieve the correct version of the work product when you need it.
In configuration management, the work products created during product development are managed using data management, version management, or baseline management. Data management is to store data in a specific location to prevent unintended changes or deletions. Version management is to record the version number and change history for each revision, and to store it in a specific location so that the work products of each version can be distinguished and retrieved. Baseline management is the management and storage of a group of work products at the time when the baseline, which is the completion reference point set in the plan, is met in a specific location so that they can be retrieved separately. The configuration management procedure is to clearly and specifically define a configuration management method at the planning stage, and during development, work products are managed at any time according to the established method, and a third party conducts a configuration audit at a specific time. The flow

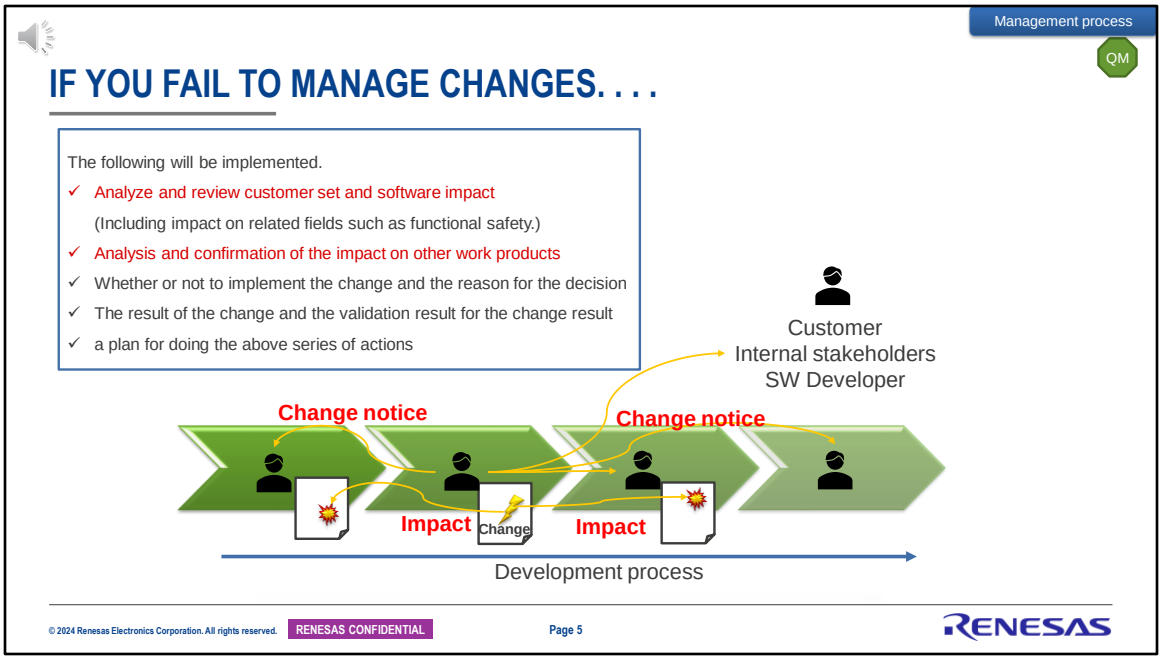
is to carry out. In configuration management, regardless of the management type, it is important to be able to identify work results and ensure reproducibility.



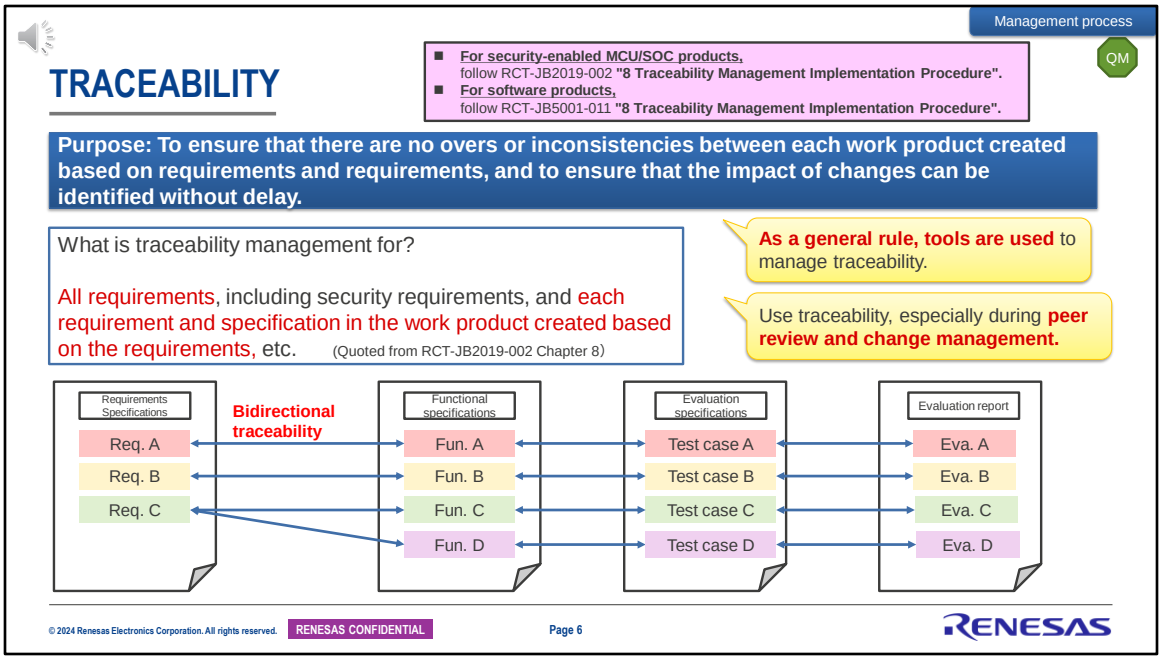
For example, in release database management, if you forget to include the RTL in the baseline of a provisional net release, and you have to go back to the provisional net and make corrections, it is difficult to know which version of the RTL should be corrected. To prevent this from happening, clarify the work products included in each baseline and verify that all necessary work products are included when creating a baseline.



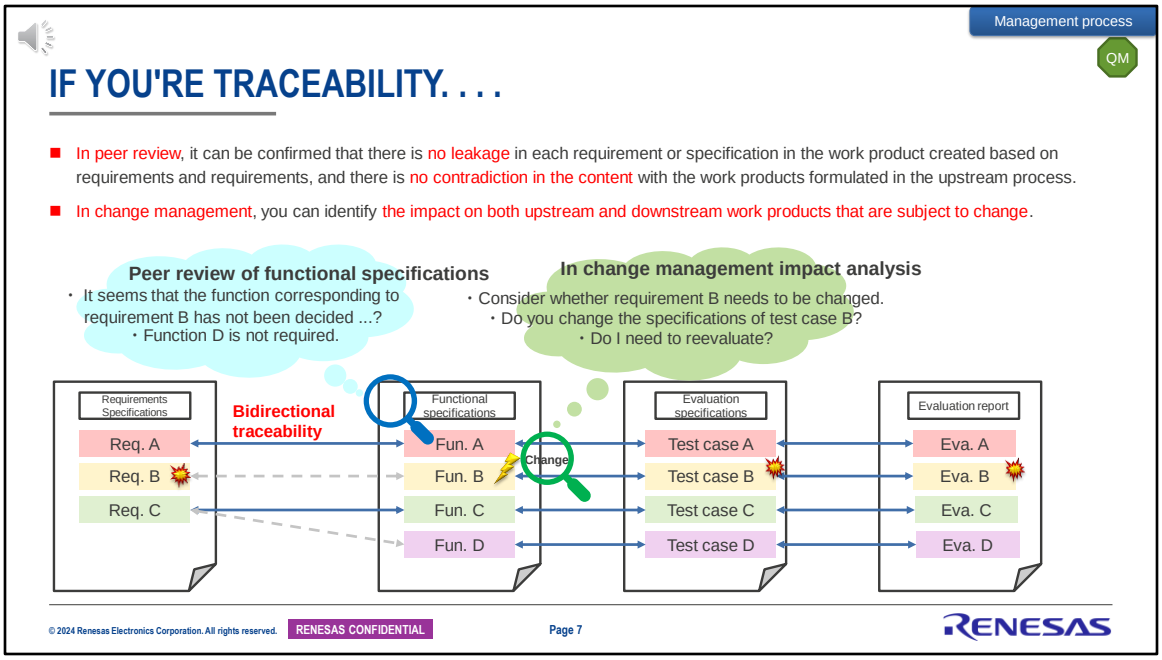
Next is change management.
The purpose of change management is to ensure that change requirements are implemented without creating conflicts between the requirements and the work products created based on them.
Change management:
We analyze the impact on the customer set and related hardware and software, as well as the impact on associated work products.
At this time, we also ask the people in charge of each field to analyze the impact on related fields such as functional safety.
Next, use the analysis results to decide whether or not to implement changes and clarify the reasons for that decision.
If we decide to make a change, we will implement the change and confirm the verification results of the change. In change management, it is important to keep records from change request to change completion.



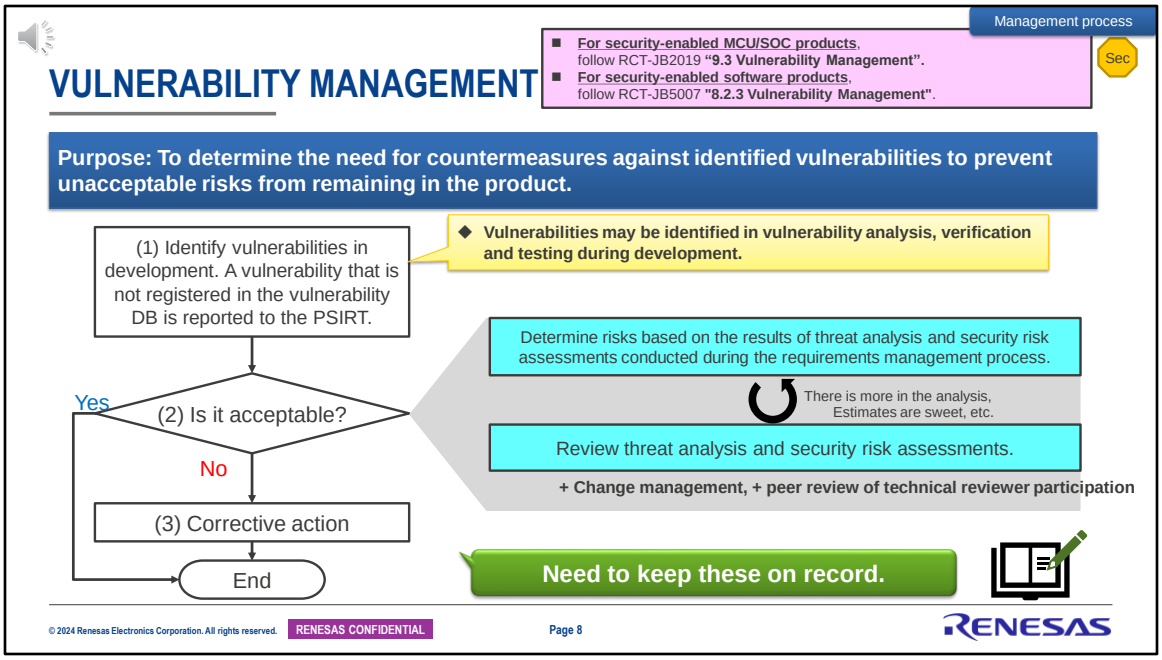
For example, neglecting impact analysis during change management can lead to inconsistencies in specifications between each work product, and broken interfaces with customer sets and related hardware and software.
Impact analysis is one of the important matters in change management, so please use traceability information, interface information, etc. to identify the scope and details of the impact of the change request.



Next is traceability.
The purpose of traceability is to confirm that there are no excesses, deficiencies, or inconsistencies between each work product created based on requirements, and to be able to fully identify the impact of change requests as explained earlier.
Traceability associates all requirements, including security requirements, with each requirement, each specification, evaluation items, or evaluation results, within the work products created based on the requirements. In principle, use traceability tools to implement traceability.



For example, by ensuring traceability, you can prevent omissions in specifications, implementation, and evaluation of requirements. Additionally, as mentioned earlier in the discussion of change management, it becomes easier to identify the impact of changes.



Next is vulnerability management.
The purpose of vulnerability management is to prevent unacceptable risks from remaining in products by determining the need for countermeasures against identified vulnerabilities.
Vulnerabilities can be detected through vulnerability analysis, verification, and evaluation during development. When a vulnerability is detected, first check whether the detected vulnerability is registered in our vulnerability database.
If it is registered in the database, we will take the corrective actions listed in the database. If it is not registered in the database, please report the vulnerability information to PSIRT.
At the same time, we compare the detected vulnerabilities with the threat analysis risk assessment results conducted in the requirements management process to determine the risk level and determine whether or not it is acceptable.
If the risk is unacceptable, develop remedial measures and take corrective actions to reduce the vulnerability below the risk tolerance.
Then, we will report the corrective measures taken and the results again to PSIRT.

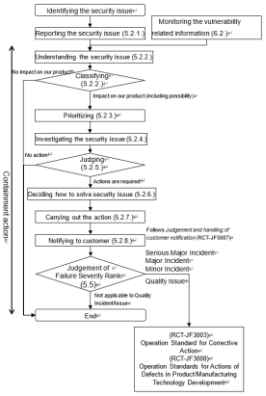
In vulnerability management, it is important to keep a record of everything from vulnerability detection to the end of the incident.

Management process

Sec

PROCEDURE FOR CORRECTIVE ACTION OF VULNERABILITIES

"Operation Standard for Action of the Security Incident and Vulnerabilities" (RCT-JF3009)



Action for security issue flowchart

Role and Responsibilities of PSIRT

- ✓ Responsible for conduct containment action on security issues.
- ✓ Determine the need to investigate reported security issues and security issues grasped through periodic monitoring, formulate or support the formulation of containment action plans, and monitor the execution of containment actions.
- ✓ Responsible for leading continuous improvement activities for security issues.
- ✓ Conduct periodic monitoring of external vulnerability-related information, periodic review of corrective actions for security issues, and in-house education.

Established HPCSG-PSIRT, EPSG-PSIRT, and PSIRT for each business body, Working in cooperation with each other.

HPCSG PSIRT:
https://renesasgroup.sharepoint.com/sites/EI/ABUSecurity_oricess_DB/Pages/ABU-PSIRT.aspx

EPSG PSIRT:
https://renesasgroup.sharepoint.com/sites/REL-MCUPD-PSIRT

RENESAS CONFIDENTIAL
Page 9

For detailed vulnerability handling procedures, please refer to the Operation Standard for Action of the Security Incident and Vulnerabilities, RCT-JF3009, which specifies the handling flow.
Please note that our company has established HPCSG PSIRT and EPSG PSIRT for each business entity, and they operate in coordination with each other. The vulnerability database is common.

Management process

Sec

SECURITY ASSET MANAGEMENT

- Follow “Operation Standard for Security Assets Management” (RCT-JB0026).

Purpose: To maintain the confidentiality, integrity, and availability of design assets.

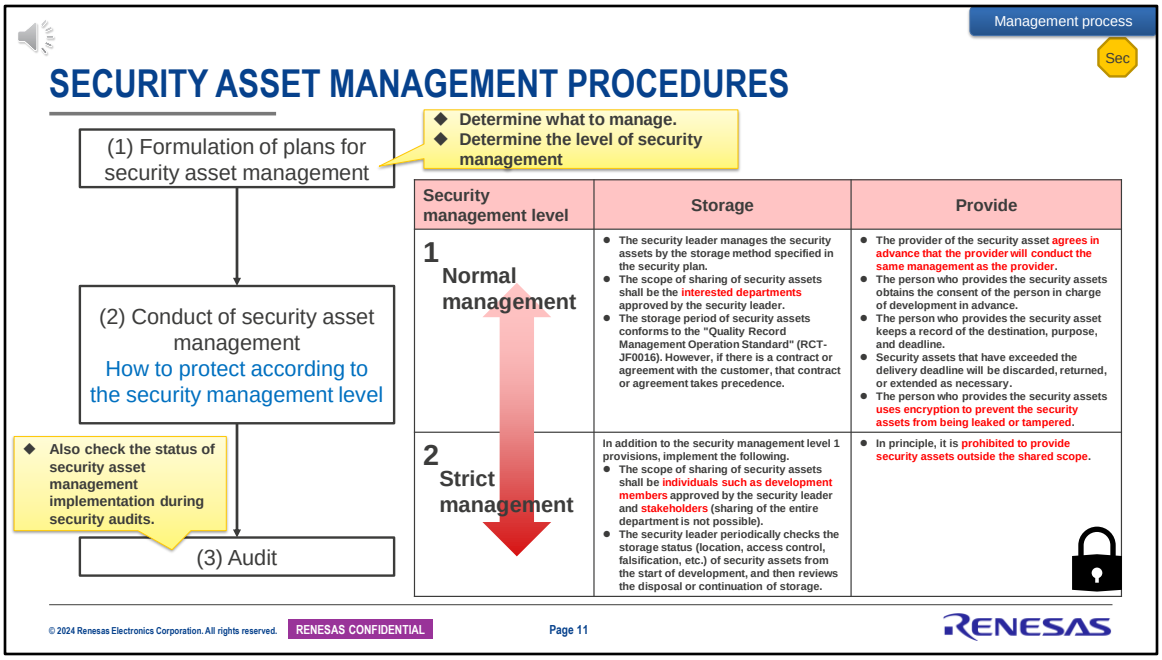
The following three are also called CIA taking the initials of English.

（Source：ISO/IEC 27000）

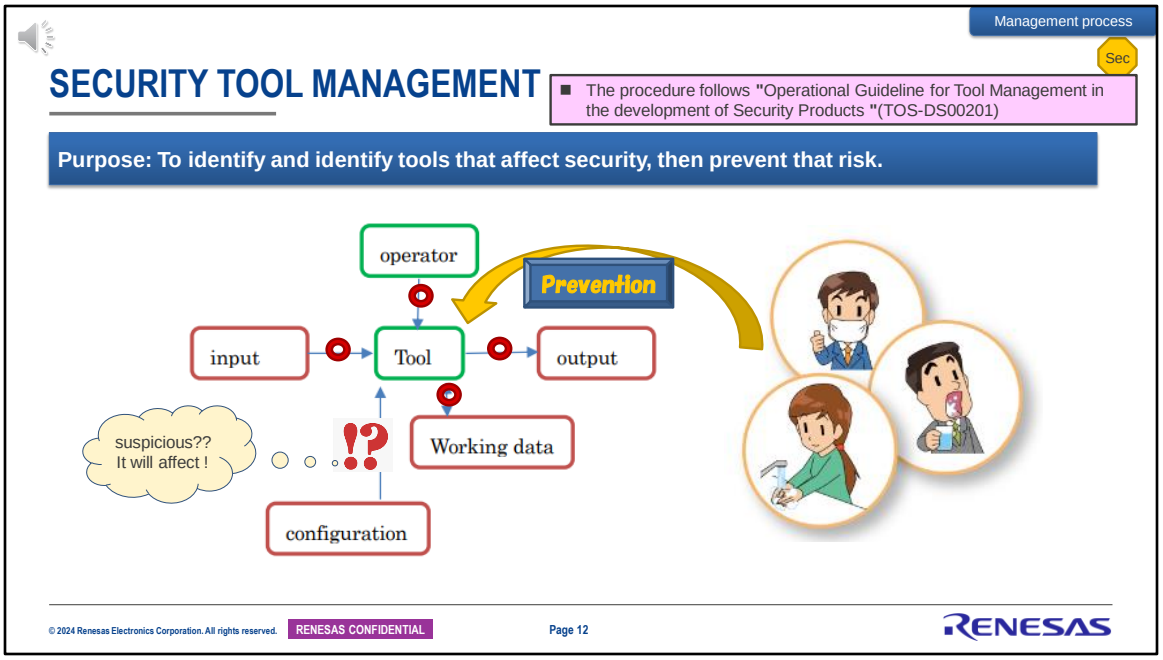
- **Confidentiality**: Ensure that only those who have access to the information have access to it.
- **Availability**: Ensure that a person who has been granted access to information has access to information and related assets without interruption when necessary.
- **Integrity**: Ensure that information has not been destroyed, tampered with or erased.

How do you protect design assets and technical information?

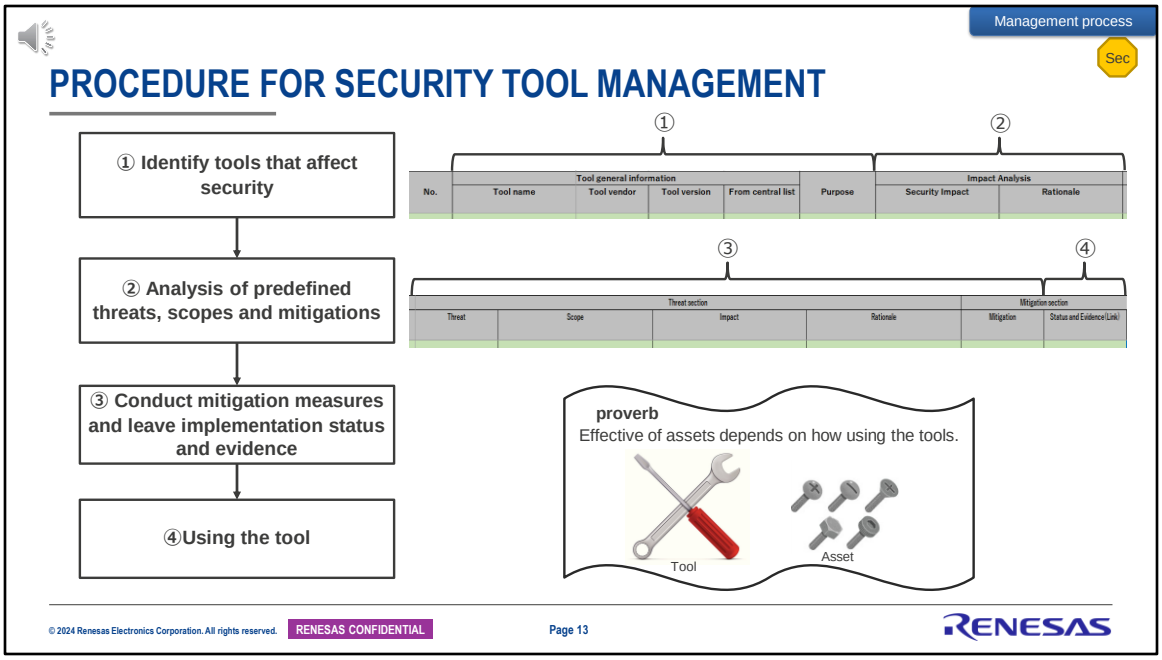
Next is security asset management.
The purpose of security asset management is to maintain the confidentiality, integrity, and availability of security design assets.
Confidentiality means ensuring that only those authorized to access the information have access to it.
Availability, in turn, is about ensuring that those authorized to access the information have uninterrupted access to the information and related assets when needed.
Finally, integrity means ensuring that information has not been destroyed, altered, or erased.



The procedure for security asset management is to create a security asset management plan during the planning stage, including deciding what to manage and building a protected environment, and during development to maintain protection of security assets based on the plan. Then, the status of security asset management will be audited by a third party at a specific time. The details of security asset management are explained in detail in the security asset management section of the security process introduction education.



Next is security tool management.
The purpose of security tool management is to identify tools that impact the security functions you implement and prevent the risk of that impact.
Security tool management begins with investigating whether the tools you use have the potential to impact the security features you implement.
For each tool you use, consider the impact on the security functions you implement from various perspectives, including input/output, operators, operating procedures, tool configuration information, and tool work data.

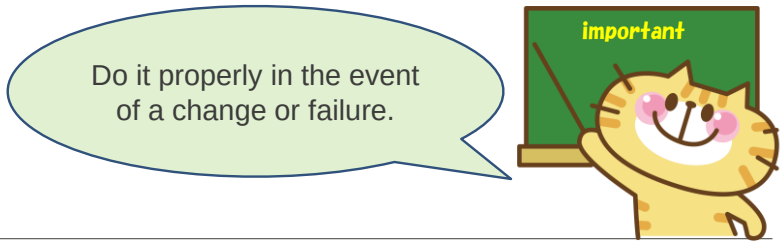


We will explain the security tool management procedure.
Using the form attached to TOS-DS00201, the technical standard for security tool management, identify whether or not the tool will affect the security functions to be implemented before using the tool.
Examples of tools include:
・Tools used for concept and product development, such as compilers, static checkers, and verification tools.
・Tools used during device evaluation such as debuggers.
・Tools used during device manufacturing such as flash programmers and testers. Etc.
Next, if it is determined that there will be an impact, we will analyze the degree and scope of the impact, formulate and record the analysis results and mitigation measures to minimize the impact.
Then, implement the developed mitigation measures and remove the risk of impact on security functions.
At this time, be sure to keep a record of the implementation or the application of the mitigation measures.
By doing this, you will be able to use security tools during development.

This concludes the explanation of the management process.

SUMMARY OF MANAGEMENT PROCESSES

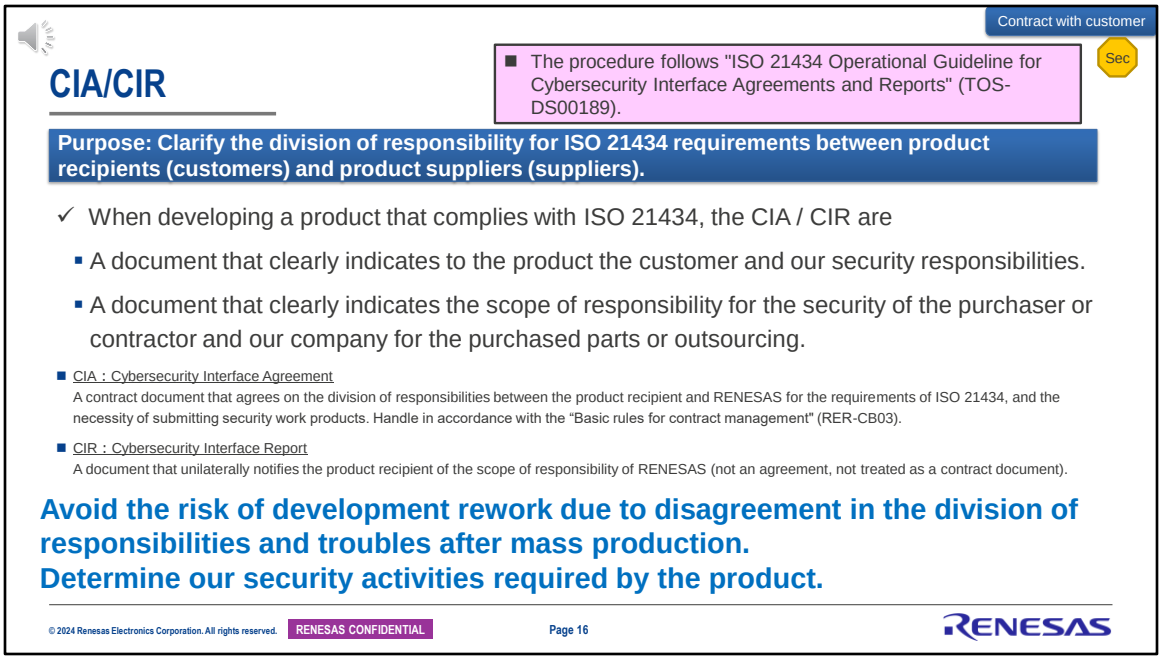
Conduct basic configuration management, change management, and traceability management correctly, and then vulnerability management, security asset management and tool management.



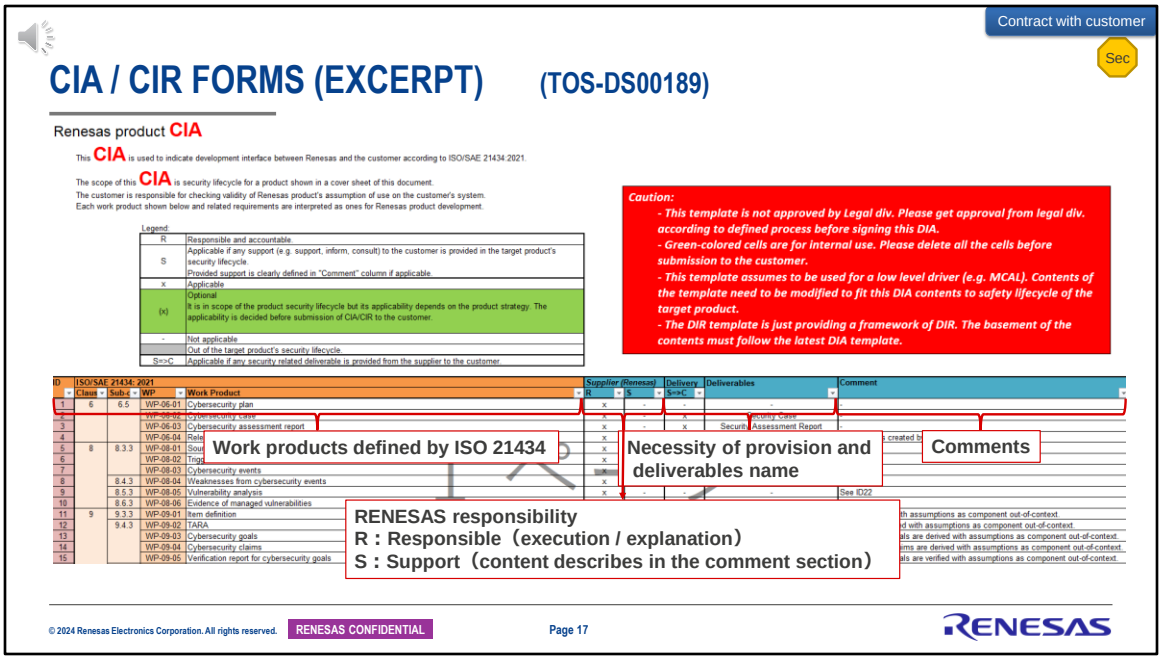
Summary of management processes.
After properly implementing basic configuration management, change management, and traceability management, we perform vulnerability management, security asset management, and security tool management.
It is important to keep accurate records of any management process.

Next, we will move on to an explanation of customer contracts and supplier selection.

5. Contract with customer, and supplier selection.



First, there is the contract with the customer.
We refer to contracts with customers for products that comply with ISO 21434 as CIA and C I R.
CIA and CIR apply only to automotive security products.
The purpose of CIA and CIR is to clarify the division of responsibility for ISO 21434 requirements between customers and suppliers. CIA and CIR are documents that clarify the scope of responsibility for security implemented in products, and are applicable to customers selling products, purchasing suppliers, and subcontractors. In other words, please understand that CIA and CIR are the security versions of DIA and DIR for functional safety for automobiles. The handling of CIA and CIR is stipulated in detail in the technical operation specification, TOS-DS00189, and the respective forms are also in place.



From the left side, the format is the work products defined in ISO 21434, the person responsible for those work products, and the name of the deliverable. CIA agrees and enters into a contract with the customer, supplier, or subcontractor regarding who is responsible for each work product. On the other hand, the CIR only informs the customer of who is responsible for each work product. A CIR is a notification and not an agreement, so it does not constitute a contract.

Supplier selection

SELECTION OF DESIGN OUTSOURCING

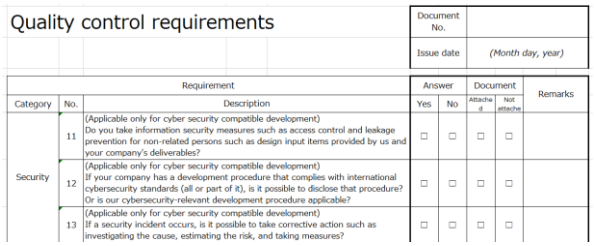
- The procedure follows "Operation Standard for Quality Control of Design Consignment" (RCT-JB0016).
- In the case of IP purchase, follows the "Implementation Standard for IP (Design Asset) Purchase " (RCT-JB1004-002).

QM

Purpose: Confirm the availability of security measures and select an outsourcer for design work.

◆ When designing and outsourcing part or all of security product development to non-affiliated companies in Japan and overseas, use RCT-JB0016 Form 1 “Quality Requirements Confirmation Form” to confirm the security maintenance status of the outsourced candidate.

◆ If there is an item that requires improvement in the result of checking the security maintenance status, perform the ordering procedure including the measures for the improvement item.



Quality control requirements

Document No.	
Issue date	(Month day, year)

Requirement			Answer		Document		Remarks
Category	No.	Description	Yes	No	Attached	Not attached	
Security	11	(Applicable only for cyber security compatible development) Do you take information security measures such as access control and leakage prevention for non-related persons such as design input items provided by us and your company's deliverables?	□	□	□	□	
	12	(Applicable only for cyber security compatible development) If your company has a development procedure that complies with international cybersecurity standards (all or part of it), is it possible to disclose that procedure? Or is our cybersecurity-relevant development procedure applicable?	□	□	□	□	
	13	(Applicable only for cyber security compatible development) If a security incident occurs, is it possible to take corrective action such as investigating the cause, estimating the risk, and taking measures?	□	□	□	□	

The next step is to select a design subcontractor. The purpose of selecting a design subcontractor for security product development is to confirm the ability of the subcontractor to implement the security requirements that we require of the subcontractor, and to select an appropriate subcontractor for the design work.
When outsourcing some or all of our security product development, please use Form 1 of RCT-JB0016 and the Quality Requirements Confirmation Form to confirm the security capabilities and maintenance status of the potential subcontractor.
Based on the confirmation results, please select a subcontractor that can meet our security requirements. If there are any items in the survey results that require improvement at the selected subcontractor, please complete the purchasing specifications and outsourcing contract, including the measures for improvement.

Finally, a summary.

SUMMARY

- Security product development consists of **regular development and security development work**. Make sure that the results of regular development and the results of security development work **do not deviate from each other**.
- Develop with an **awareness of the purpose** of each security development work.
- It is necessary to conduct the management process not only during development **but also after the development is completed**.

First, security product development consists of a combination of regular development and security development. It is important to promote development so that the results of regular development and security development do not diverge.
Second, please be aware of the purpose of each security development when proceeding with development.
Third, management processes need to be implemented not only during development, but also after development is complete.

With this, we conclude the security product development process of the Renesas security process introduction. Thank you for listening.

Rev.	Date	Approval/making	Contents
0.9	2020/10/15	Nagata/Fujii	New
1.0	2020/12/18	Nagata / Amimoto / Fujii	・Review of contents according to TOS-DS00146 Ver.1.0 ・RCT-JB0026 Review of contents according to 1st edition
1.1	2020/12/21	Nagata / Amimoto / Fujii	5. Refer to the management process Added technical standards to be
1.2	2021/01/21	Nagata/Fujii	P2,3 Changed training module from 5 to 4
2.0	2022/03/02	Nagata/ Fujii, Amimoto	Updated contents according to TOS-DS00146 3rd edition, RCT-JB2019 3rd edition, RCT-JB5007 3rd edition
3.0	2024/06/03	Nagata/ Fujii, Amimoto	Added vulnerability analysis/management process and reflected feedback from TUV audit

Thank you